REMARKS

Applicants appreciate the thorough review of the present application reflected in the Office Actions dated December 8, 2005, May 26, 2006 and October 31, 2006, as well as the withdrawal of the rejections of Claims 1-9 and 14-28 as being anticipated by U.S. Patent No. 5,191,611 to Lang. For the reasons discussed herein, Applicants respectfully request reconsideration of the newly raised rejections under 35 U.S.C. § 103 for the reasons discussed below.

I. Independent Claims 1, 14 and 19

Independent Claims 1, 14 and 19 are directed to, respectively, a method, a system and a computer program product for selectively allowing access to a plurality of resources in a network. The Office Action states that each of Claims 1, 14 and 19 is obvious over U.S. Patent No. 5,548,649 to Jacobson ("Jacobson") in view of U.S. Patent No. 6,366,912 to Wallent et al. ("Wallent"). (Office Action at 2-4). In particular, the Office Action states that Jacobson discloses all of the recitations of Claims 1, 14 and 19 except for the "level of security sensitivity of the resource, and that this missing teaching is provided by Wallent. (Office Action at 4). Applicants respectfully traverse the rejections of Claims 1, 14 and 19 for at least the four (4) independent reasons discussed in the following subsections. The arguments below are presented with respect to Claim 1, but it will be understood that due to the correspondence between Claims 1, 14 and 19, each of these arguments apply equally against the rejections of Claims 14 and 19.

Claim 1, which is representative of Claims 1, 14 and 19, recites:

> 1. A method for selectively allowing access to a plurality of resources in a network, the method comprising:
>
> receiving a request originated from a user of a multi-user system to transmit a message via the multi-user system over the network to one of the plurality of resources, wherein each of the plurality of resources has been assigned to one of a plurality of security zones based on a level of security sensitivity of the resource;

identifying a one of the plurality of security zones that is associated with the one of the plurality of resources;

determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones; and

forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the identified one of the plurality of security zones.

The Office Action states that (1) the "host devices 102-1 through 102-10 of Jacobson comprise the "resources" of Claim 1, (2) the security bridges 104-1 through 104-3 of Jacobson each correspond to the "multi-user system" of Claim 1, (3) that secure zones 108-1 through 108-3 comprise the "plurality of security zones" recited in Claim 1, and (4) that Figure 1 of Jacobson shows each of the "resources" (host devices) being assigned to one of the security zones. (Office Action at 3). As shown in the following sections, however, Jacobson fails to disclose several of the recitations of Claim 1, and Wallent is neither cited as disclosing, nor discloses, the recitations of Claim 1 that are missing from Jacobson. Accordingly, Applicants respectfully submit that the Office Action fails to make a *prima facie* rejection of Claims 1, 14 and 19 under 35 U.S.C. § 103(a), and hence, the rejections of Claims 1, 14 and 19 should be withdrawn.

A. Jacobson Does Not Disclose Identifying a Security Zone that is Associated with a Resource to which a Message is to be Sent

The second clause of Claim 1 recites "identifying a one of the plurality of security zones that is associated with the one of the plurality of resources." The Office Action states that Jacobson discloses grouping the host devices 102-1 through 102-10 into the plurality of secure zones 108-1 through 108-3. (Office Action at 3). While Applicants agree that Jacobson does in fact group the host devices 102-1 through 102-10 into the plurality of secure zones 108-1 through 108-3 (or into an unsecure zone), this is not what is recited in the second clause of the body of Claim 1. Instead, what the combination of the first two clauses of the body of Claim 1 recite is "identifying a . . . **security zone that is associated with the resource" (herein the**

"identifying" recitation) for which a request to transmit a message has been received. Jacobson does not attempt to identify a particular one of the security zones 108-1 through 108-3 in response to receiving a request to transmit a message. Instead, as discussed in the Office Action, Jacobson merely discloses grouping resources into a plurality of zones. Thus, the rejection of Claim 1 should be withdrawn for at least this reason.

B. Jacobson Does Not Determine if a User is Authorized Access to an Identified Security Zone

The third clause of the body of Claim 1 recites "determining if the user of the multi-user system is authorized access to the identified one of the plurality of security zones" (herein the "determining recitation" of Claim 1). The Office Action states that the "identification filter table" at each security bridge 104-1 through 104-3 of Jacobson is "used to identify if the request [sic] transmitted packet is authorized to access one of [the] security host device[s]." Applicants note that Jacobson does not describe any "identification filter table" as stated in the Office Action, but instead discusses several "filter tables" and several other "identification tables." While the Office Action does not clearly indicate which of these tables forms the basis for the pending rejection of Claims 1, 14 and 19, Applicants respectfully submit that the discussion below demonstrates that none of these tables disclose the "determining" recitation of Claims 1, 14 or 19.

In particular, the various "filter tables" described in Jacobson are the Ethernet protocol filter table 214, the IP protocol filter table 220, the IP address filter table 222. (Jacobson at Col. 6, lines 4-65). Jacobson does not disclose or suggest that these "filter tables" are used to "determine[e] if **the user** of the multi-user system is **authorized access to the identified one of the plurality of security zones**" as recited in the third clause of the body of Claim 1. Instead, the filter tables of Jacobson appear to be used to determine if a "normal data packet has been received" and if not, the packet is deleted. (*See, e.g.,* Jacobson at Col. 6, lines 13-28). There is simply no disclosure or suggestion in Jacobson that the "filter tables" filter based on whether or

not a **user is authorized access to a particular security zone**. To the contrary, filter tables 214 and 220 appear to **filter based on the protocol types of particular packets**, while filter table 222 appears to filter out packets with IP addresses associated with particular hosts and/or bridges, but does so **without reference to any particular security zone**. (*See, e.g.*, Jacobson at Col. 6, lines 7-19, 41-48 and 62-65). In fact, the exemplary "filter tables" disclosed in Figures 6-8 of Jacobson clearly show that the filtering is performed **solely** on either protocol types or IP addresses as opposed to based on whether or not a user is authorized access to a particular security zone. Thus, the discussion of the "filter tables" of Jacobson fail to disclose or suggest the "determining" recitation of Claim 1.

Similarly, the two "identification tables" discussed in Jacobson – namely the remote secure zone host identification table 230 and the local secure zone host identification table 236 – are not used to "determine[e] if the user of the multi-user system is authorized access to the identified one of the plurality of security zones" as recited in the third clause of the body of Claim 1. Instead, the identification tables 230 and 236 are used in determining the source and/or destination zone of a particular packet in order to determine, for example, whether encryption and/or decryption operations should be performed on the packet. The description at Columns 7 and 8 of Jacobson thus clearly shows that neither identification table 230 nor identification table 236 are used to determine if a user is authorized access to a security zone, let alone to determine if a user is authorized access to an **identified** security zone that is associated with the resource to which the user is sending a message as recited in Claim 1. Accordingly, the rejection of Claim 1 should also be withdrawn for this reason.

C. Jacobson Does Not Disclose Forwarding a Message Only if it is Determined that the User is Authorized Access to the Identified Security Zone

The last clause in the body of Claim 1 recites "forwarding the message from the multi-user system over the network only if it is determined that the user is authorized access to the

identified one of the plurality of security zones." The Office Action states that Col. 7, lines 1-67, Col. 8, lines 1-48 and Col. 15, lines 1-15 of Jacobson discloses this recitation of Claim 1. (Office Action at 4). In particular, the Office Action states that the security bridges 104-1 through 104-3 of Jacobson forward "authorized install/or view request" packets – which are deemed to be the equivalent of the "message" of Claim 1 – to the desired security zone host device 102-1 through 102-10. (Office Action at 4). Applicants respectfully submit that the cited portions of Jacobson also fail to disclose the last clause of Claim 1 for at least two separate reasons.

As an initial matter, what the last clause of Claim 1 recites is that the message is forwarded "only if it is determined that the **user is authorized access to the identified . . . security zone**." In contrast, the cited portion of Jacobson states that the local bridge "determines if the user is authorized to install or view the item in the local bridge in a manner similar to that described earlier for determining from the distribution authorization request packet if the user is authorized to distribute an item to a remote bridge." (Jacobson at Col. 15, lines 21-25). The earlier referenced portion of Jacobson, in turn, recites:

> [T]he bridge manager determines whether the user is authorized to perform the bridge local install or view operation. This is done by comparing the user's i.d. and password for accessing local bridge 104-1 with those stored in authorization table 244 and looking up the user's authorization level in the authorization table 244.

(Jacobson at Col. 10, lines 22-28). Thus, in Jacobson, whether or not a user is allowed to install or view items contained in the bridge library 216 is based on whether the user – as identified by an i.d. and a password – has a sufficient **authorization level** as opposed to being based on a determination as to whether or not the user is authorized access to **an identified security zone** (i.e., a security zone that has been identified as being associated with the resource to which the message is being sent) as recited in Claim 1.

More importantly, the network management operations described in Column 15 of Jacobson for installing and/or viewing items in the bridge library are operations that are

performed by the "user" of Jacobson. (*See* Jacobson at Col. 15, line 6). As noted above, Jacobson states that these operations are performed in a manner similar to bridge management operations described earlier in Jacobson. (Jacobson at Col. 15, lines 22-26). The earlier description of the bridge management operations makes clear that the "user" referred to in Jacobson is "user 246" which is depicted in Fig. 2.[1] As shown in Fig. 2, the **user terminal 246 is part of** the network security bridge 104-1. Accordingly, the operations for viewing and/or installing items in library 216 have nothing to do with **receiving a request from a user of a multi-user system to transmit a message over a network** as recited in Claim 1, but instead involve a user performing management operations on security bridge 104-1 by logging onto a user terminal present at the security bridge. Accordingly, Jacobson fails to disclose or suggest the last clause of Claim 1 for this independent reason.

Thus, for each of the above reasons, Applicants respectfully submit that the rejections of Claims 1, 14 and 19 should be withdrawn. Applicants also respectfully submit that one of skill in the art would not have been motivated to combine Jacobson and Wallent in the manner suggested in the pending rejections. However, in light of the clear showing above that the combination of Jacobson and Wallent fail to disclose numerous of the recitations of Claims 1, 14 and 19, Applicants will not detail here the reasons that one of ordinary skill in the art would not have sought to combine Jacobson and Wallent in the manner suggested.

II. Independent Claim 24

The Office Action states that Claim 24 is rejected for the same reasons that Claim 1 was rejected. (Office Action at 4). Thus, the rejection of Claim 24 should be withdrawn for various of the reasons, discussed above, that the rejection of Claim 1 should be withdrawn (to the extent Claims 1 and 24 share common recitations). In addition, Claim 24 contains different recitations

---

[1] Fig. 2 of Jacobson includes a typographical error in that the "user terminal" is labeled 248 and the "serial interface" is labeled 246, whereas in the text of Jacobson the user is referred to as "user 246" and the serial interface is referred to as "serial interface 248."

than does Claim 1, and hence Claim 24 cannot properly be rejected without addressing the specific recitations included therein. For example, the Office Action does not explain where Jacobson discloses "receiving a message over the network from one of the plurality of resources that is addressed to a process running on the multi-user system that is associated with the user" as recited in the first clause in the body of Claim 24. Applicant respectfully submits that Jacobson does not disclose this recitation of Claim 24, and hence the rejection of Claim 24 should also be withdrawn for this additional reason. In any event, the Office Action has clearly not addressed the different recitations included in Claim 24, and hence has failed to make a *prima facie* rejection of Claim 24.

III. Independent Claim 25

Claim 25 recites:

> 25. A data processing system for selectively allowing access to a plurality of resources in a network, comprising:
> a data processing device, the data processing device connected to a first network that includes a plurality of networked resources;
> a plurality of workstations that are configured to execute applications on the data processing device;
> a first data structure that specifies at least one security zone from a plurality of security zones that is associated with each of the plurality of networked resources, wherein each of the plurality of security zones represents a distinct level of security sensitivity; and
> a second data structure that specifies the respective security zones to which a plurality users of the data processing device may have access.

The Office Action states that the "host devices" of Jacobson are equivalent to the "data processing device" of Claim 25; that the "remote security zone Host ID table" comprises the "first data structure" of Claim 25; that the "authorization table" of Figure 12 of Jacobson comprises the "second data structure" recited in Claim 25, and that "communications between the host devices" comprise the plurality of workstations recited in Claim 25. (Office Action at 5).

Applicants also respectfully submit that the cited portions of Jacobson do not correspond to the recitations of Claim 25.

For example, the rejection of Claim 25 indicates that the host devices comprise the "data processing device" of Claim 25 and that communications between the host devices comprise the "plurality of workstations" of Claim 25. What Claim 25 recites, however, is a "plurality of workstations that are **configured to execute applications on the data processing device**." Applicants respectfully submit that the cited portions of Jacobson do not indicate that the host devices are configured to execute applications on each other and, as such, communications between the host devices does not disclose or suggest the "plurality of workstations" of Claim 25. Therefore, the rejection of Claim 25 should be withdrawn for at least this reason.

Applicants also submit that the Host ID table of Jacobson does not correspond to the "first data structure" of Claim 25. The remote secure zone host ID table, which is depicted in Figure 9 of Jacobson, maps the IP address of host devices 102-3 through 102-7 to their corresponding security bridge 104-2 or 104-3. (Jacobson at Col. 7, lines 25-33). As such, the host ID table maps the host devices to a particular **security bridge** as opposed to mapping networked resources to particular **security zones**, and hence does not correspond to the "first data structure" of Claim 25.

Applicants further submit that the "authorization table" of Figure 12 of Jacobson does not disclose or suggest the "second data structure" of Claim 25. Instead, as discussed above, the "authorization table" 244 of Jacobson specifies the types of operations that particular users may perform on a selected one of the security bridges 104-1 through 104-3. (*See, e.g.,* Jacobson at Col. 10, lines 22-28). As such, the authorization table clearly does not specify the respective security zones to which a user may have access, as can clearly be seen by viewing the last column in the authorization table of Figure 12. Thus, the failure of Jacobson to disclose the second data structure provides a third, independent basis for withdrawal of the rejection of Claim 25.

Thus, for each of the above reasons, Applicants respectfully submit that the rejection of Claim 25 should also be withdrawn.

IV. The Dependent Claims

Each of the remaining claims depend from one of Claims 1, 14, 19, 24 or 25, and hence is patentable over the cited art for at least the reasons that the claim from which it depends is patentable. As several bases have already been identified for withdrawal of the rejections of each independent claim, Applicants will not here identify the additional reasons that various of the dependent claims are further patentable over the cited art.

V. Conclusion

For each of the above reasons, Applicants respectfully submit that the pending claims are patentable over the cited art, and respectfully request the present application be passed to issuance.

Respectfully submitted,

D. Randal Ayers
Registration No. 40,493

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401